Prof. Dr. Bürgisser
Paul Breiding

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Multivariate Polynomials

Sommersemester 2015

Exercise session 2

Exercise 1. Let the arithmetic circuit Φ be represented by the graph below. Determine $|\Phi|$, $D(\Phi)$ and the polynomials $\widehat{\Phi}_v$ for all gates v.

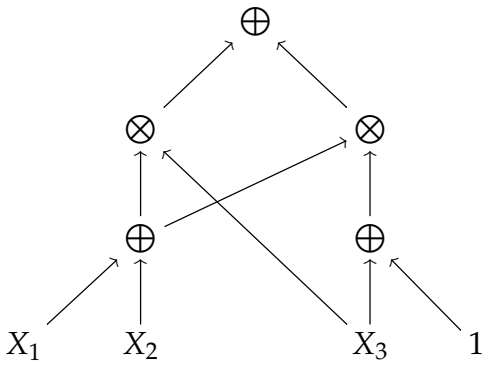

Figure 1: Graph representation for Φ.

Exercise 2. For $n \geq 1$, put $[n] := \{1, \ldots, n\}$. Let f_n denote the following polynomial in the $3n^2$ variables $(x_{i,j})_{1 \leq i,j \leq n}$, $(y_{i,j})_{1 \leq i,j \leq n}$ and $(z_{i,j})_{1 \leq i,j \leq n}$.

$$f_n := \sum_{(i,j) \in [n] \times [n]} z_{i,j} \cdot \left(\sum_{k \in [n]} x_{i,k} \cdot y_{k,j} \right).$$

Let $\omega \geq 2$. Show that, if the product of two $n \times n$-matrices can be computed by arithmetic circuits of size $\mathcal{O}(n^\omega)$, then $L(f_n) \in \mathcal{O}(n^\omega)$.

Exercise 3. Prove the lemma from the lecture:
Let $f \in \mathbb{K}[X_1, \ldots, X_n]$ and suppose that there exists an arithmetic circuit Φ with r multiplication gates that computes f. Then there exists a sequence $(g_1, \ldots, g_r)$ in $\mathbb{K}[X_1, \ldots, X_n]$ with the following property:
For all $1 \leq \varrho \leq r$ there exist $u_\varrho, v_\varrho \in \operatorname{span}_{\mathbb{K}} \{1, X_1, \ldots, X_n, g_1, \ldots, g_{\varrho-1}\}$, such that $g_\varrho = u_\varrho \cdot v_\varrho$ and $f \in \operatorname{span}_{\mathbb{K}} \{1, X_1, \ldots, X_n, g_1, \ldots, g_r\}$.

Prof. Dr. Bürgisser
Paul Breiding

Technische Universität Berlin
Fakultät II, Institut für Mathematik
Sekretariat MA 3-2

Exercise 4. Consider the multivariate polynomial

$$f = \sum_{e \in \{0,1\}^n} f_e \cdot X_1^{e_1} \cdot \ldots \cdot X_n^{e_n} \in \mathbb{K}[X_1, \ldots, X_n].$$

Let $L^{\times}(f)$ denote the number of multiplications sufficient to compute f from the input set $I := \mathbb{K} \cup \{X_1, \ldots, X_n\}$. If we only count non-scalar multiplications, we get the non-scalar complexity $L^{\mathrm{ns}}(f)$. Prove:

(1) $L^{\times}(f) \leq 2^n - 1$.

(2) $2^{\frac{n}{2}} - n \leq L_{\mathrm{ns}}(f)$.

(3) $L^{\mathrm{ns}}(f) \leq 2^{\frac{n}{2}+1}$.

Hint: For part (3) divide the variables $X_1, \ldots, X_n$ into two groups $Y_1, \ldots, Y_{\lceil \frac{n}{2} \rceil}$ and $Z_1, \ldots, Z_{\lfloor \frac{n}{2} \rfloor}$ and express f as polynomial in the Y_i. Then use induction.